TITLE: Analyzing Economic Espionage

AUTHOR: (b)(3)(c)

VOLUME: 36 ISSUE: Spring YEAR: 1992

STUDIES IN INTELLIGENCE

A collection of articles on the historical, operational, doctrinal, and theoretical aspects of intelligence.

A foreign intelligence threat

Analyzing Economic Espionage

(b)(3)(c)

This article was the basis for testimony given on 29 April 1992 by the Director of Central Intelligence before the Subcommittee on Economic and Commercial Law, Committee on the Judiciary, House of Representatives. An earlier version of the article appeared in the November 1991 issue of Counterintelligence Trends.

Analyzing the foreign intelligence threat to US economic interests—not to mention countering it—is difficult. The threat is diffuse, and it comes primarily from countries whose intelligence activities we have not tracked closely. It is complex, and it is characterized by a wide variety of operational practises not easily classified in accordance with conventional categories of espionage activity.

The Changing Threat

With the end of the Cold War, the foreign intelligence threat has become less concentrated. The winding down of international military competition, the declining perception that the Free World faces a common threat, and the growing tendency to measure national power and national security in economic as well as military terms are causing countries everywhere to reassess their intelligence priorities.

Foreign targeting of American technology continues; technology is important for economic as well as military reasons. Because the US continues to be on the cutting edge of technological innovation—leading even the Japanese in this respect—technology theft will remain a major concern for the US. Requirements of individual intelligence services are of course influenced by the particular economic needs of each country. But, in general, those areas of technology critical to any country's ability to compete effectively internationally, especially those areas where the US maintains a lead, are most vulnerable. These areas include aircraft and space technology, biotechnology, data processing, and advanced manufacturing. Companies leading in research development and product commercialization in these technologies are prime targets for foreign intelligence operations.

Foreign intelligence operations against our economic interests, however, encompass more than technology diversion. Some foreign governments target a range of economic and business data. They want access to US Government policy deliberations concerning foreign trade, investments, and loans, and positions on bilateral economic negotiations. Several governments also seek information about company bids for contracts and takeovers, information that affects prices of commodities, financial data, and banking information affecting stock market trends and interest rates.

In addition to collecting economic information, a few foreign intelligence services have tried to exert clandestine influence on US business and government decisions that affect their economic interests. They have attempted to recruit agents of influence in US Government, banking, and business circles. Besides those who have pushed such "active measures" in the economic area, several governments engage in aggressive lobbying on behalf of their national firms, to the point of exerting political and economic leverage in a heavy-handed manner.

Another reason the threat has become more extensive in recent years is that the number of foreign intelligence services capable of conducting sophisticated operations has increased. There has been a proliferation of commercially available intelligence technologies. In addition to technologies for intelligence operations becoming cheaper, dozens of Third World intelligence services have profited from training they

received in the past from either Western or East Bloc services, and they are now more able to act unilaterally.

At the same time, with large numbers of intelligence operatives thrown out of their jobs in some former communist countries, the reservoir of professionally trained intelligence mercenaries is growing. Some former *Stasi* officers have even taken out classified ads in German newspapers.

Categories of Countries

In an environment of heightened global economic and technological competition, and one in which intelligence capabilities have proliferated, the danger exists of intelligence operations being conducted against our economic interests from a variety of sources. First of all, those traditional adversaries that remain in business against us are giving a high priority to both technology theft and economic intelligence collection. This is true of intelligence services both in unreformed communist countries and in some reforming former communist countries. The economic distress that former communists countries are experiencing in some cases gives impetus to intelligence efforts to acquire information and advanced technology of commercial value to them. The communist governments that remain, feeling increasingly isolated and threatened by "democratic encirclement," continue to view technology theft as one means of propping up their repressive regimes, military arsenals, and sagging economies.

For many countries, collection of weapons technology serves both economic and military ends. The technology may enhance the country's military capabilities, while also making its armaments industries better able to compete with US suppliers in international arms markets. The extremely sensitive nature of the information pertaining to weapons proliferation—chemical, biological, nuclear, and ballistic missiles—has led most governments interested in procuring weapons technology to lean heavily on their intelligence services.

We also have to be alert to the activities of countries whose national intrests have been compatible with ours. In the post-Cold War world, more of our friends may adopt a parallel approach of cooperating with us in the realm of diplomacy and military liaison while engaging in intelligence practices that put them in an adversarial relationship with us. We now lack the evidentiary basis to establish any overall trend toward increased economic espionage among advanced industrial countries. Nevertheless, economic intelligence collection by such countries is potentially more damaging to our economy than intelligence operations by traditionally hostile countries, because some traditionally friendly countries are strong economic competitors, which the communist and former communist states clearly are not.

Finally, there is a category of countries that are not major economic competitors of the US across the board but are competitors in particular sectors. Collection of economic intelligence by such countries could damage those particular sectors of the US economy.

The emergence of regional trading blocs or economic associations, (b)(1) could also portend an increase in economic espionage against US interests. We have yet to see the emergence of regional intelligence services, and it is doubtful that any such supranational services will emerge in the near future. There is reason to believe, however, that in striving to develop common foreign, economic, and trade policies, members of regional groups may direct their national intelligence services to cooperate more fully—even to pool intelligence resources—in support of common goals.

Approaching the Problem

There are many gradations in the threat. Some foreign efforts to gain economic advantage through collection programs pose serious problems for the US; others do little damage. In assessing what sort of threat various activities constitute, we look at several basic questions.

First, *who* is conducting the activity? Often the primary actor from a given country is not an intelligence organization but a business or another component of the government performing *de facto* intelligence functions, such as a trade organization or economics ministry. When private firms are involved, an intelligence agency or government is sometimes sponsoring, orchestrating, or coordinating the activity. This is more likely to be the case in countries with

centralized economies or corporative structures in which there is no clear separation between public and private sectors, between business companies and government agencies.

Take, for example, the case of a scientist from a foreign private research institution who attends a professional conference in the US and picks up information from colleagues in open discussion. We consider whether the scientist is a cooptee of an intelligence service, whether he was given collection requirements, whether he had an obligation to report back to his government, and whether his trip was part of a systematic collection program. One or more of these circumstances may obtain. (Similarly, foreign governments sometimes play a role behind the scenes in facilitating visits of researchers working for foreign corporations to our federal laboratories or encouraging foreign businesses to sponsor R&D programs at American universities that provide them some degree of proprietary control over the technology through patents or licenses.)

Second, we look at *what* is being collected—the "shopping list." This may be embargoed technology or classified research. But it is important to keep in mind that much valuable information is available from open sources. Even most intelligence services, including those in former communist countries, have begun to place a higher premium on open-source collection. This is partly because advances in data processing have made it much easier to aggregate, manipulate, and exploit large volumes of data. And it is partly because open-source collection is less politically risky for services that do not want to get caught in classic espionage operations.

Third, we look at *where* the information is obtained. Foreign intelligence services are more inclined to operate against American targets outside the US. They know there is a greater chance American officials will detect an operation taking place on our own territory, and a greater likelihood of serious repercussions once the operation is detected. Most services are consequently more aggressive inside their own countries, where they can control the operating environment better and the legal environment is naturally benign. Operations against US targets in third countries constitute another approach in use.

Fourth, we consider *how* the information is acquired. In human operations, some intelligence services that stop short of recruiting US citizens use intelligence operatives to elicit information from them; the targeted American is unwitting of his interlocutor's intelligence connection.

(b)(1)

In addition to human operations, a number of services conduct technical operations against US businesses. On the low-tech end, such things as bugging hotel rooms of traveling American executives occur. Beyond such practices, we operate on the assumption that any technically sophisticated intelligence service could mount a technical attack against US businesses or businessmen in their countries. Attractive targets would be a company's communications and computer systems.

Finally, we look at *why* the information is collected and what is done with it. A number of countries, for example, disseminate economic information and some economic intelligence to individual national firms. This process is sometimes regularized, but it is also facilitated by the existence of informal channels between government and industry.

Patterns of Activity

Distinguishing between these various types of activity, we can discern several distinct collection patterns, each more or less characteristic of one or more countries today.

The first pattern—(b)(1) is classic espionage, in which a foreign intelligence organization operates clandestinely on a global basis to recruit and run paid agents in US companies and governmental institutions. This is often done by using academic, business or international organization cover, which often succeed where a straightforward pitch to work for a foreign intelligence service would fail.

In the second pattern, (b)(1) intelligence operatives rely largely on elicitation rather than outright recruitment, and often try to exploit ethnicity as a means of developing targets.

In the third pattern, (b)(1) the intelligence service conducts "bag operations" within its own border, surreptitiously entering hotel rooms of visiting American officials or executives to search for documents containing sensitive economic or business data, taking advantage of other security lapses as well, and passing the information gathered to national firms.

In the fourth pattern, (b)(1) the government operates not through intelligence services *per se* but through other components to conduct an extensive, systematic program of collecting information of economic value—largely but not entirely from open sources—and disseminating it to business leaders.

The fifth pattern (b)(1) In this case, a government covertly targets sensitive weapons technology by working through front organizations, military attaches, and special intelligence units that operate outside of regular intelligence organizations and may be directly subordinated to top national leaders. A high premium is placed on secrecy in the process of diverting the technology and on deception in preventing its acquisition from becoming known later.

An emerging sixth pattern is that of intelligence *entrepreneurs* prepared to sell their services either to foreign governments or to private organizations.

It is important for us to make these distinctions about different patterns of activities. Doing so helps in analyzing and understanding the problem. It also helps in deciding what sort of response is appropriate in particular cases. We do not have the same level of counterintelligence interest in all types of foreign collection activity. (b)(1) At the same time, it is essential that we monitor and defend ourselves against more sinister activity. Deciding what activities cross the threshold to require a vigorous response is essentially a policy decision.

Sizing the Problem

In assessing the seriousness of the threat of foreign economic espionage, it is necessary to consider whether the US has peculiar vulnerabilities to foreign intelligence operations. To gain perspective on the problem, it also is helpful to place the economic espionage threat in the larger context of foreign aggressive activities to gain economic advantage over the US through a variety of methods that seem unfair by American standards.

A strong argument can be made that the US is more susceptible than many countries to foreign intelligence machinations. It is a truism that we have an open society in which most of our business, government and commercial, is conducted in public view. We also have a fairly clear demarcation between business and government. Whether or not there is a Japan Inc. may be debated, but there is not an America Inc. These circumstances make it harder for us to defend against foreign intelligence efforts that coordinate activities of business and government. Increased foreign ownership of US companies further complicates an already difficult situation.

Moreover, it is possible that many Americans possess certain personality attributes that increase our vulnerability. (b)(1)

- (b)(1) Americans like to talk. We tend to be sociable and gregarious, even with casual contacts. We want to be liked, especially by foreigners, because many of us are still trying to overcome an "ugly American" complex. We place a higher premium on candor than on guile, on trust than on discretion.

- Many Americans do not know foreign languages, which in some respects puts them at a disadvantage when living in foreign countries. This does not mean we are "innocents abroad," but it may make us less likely to pick up clues of suspicious behavior. Americans who do not know the language of a given country may forget that nationals of that country in a position to overhear their conversations often do know English.

- Many Americans are ambitious, oriented toward job advancement and professional recognition. Inevitably, some morally weak individuals are willing to sacrifice personal integrity in pursuit of these career goals.

Our vulnerability may increase as a result of reduced US military spending, the scaling down of US national security institutions, and corresponding cuts for Department of Defense contractors. Layoffs in the American defense industry and reduced opportunities for upward mobility in government service may produce morale problems, thereby creating a "happy hunting ground" for foreign intelligence services seeking to recruit Americans in possession of sensitive information.

Espionage is only one of the destructive activities that some foreign governments resort to in order to gain advantage over US industry. Tailoring government procurement policies to favor domestic firms, manipulating standards and testing regulations to the detriment of foreign firms, under-the-table subsidies, schemes to promote or illegally dump exports or to choke imports, barter and other countertrade activities are all examples of such market-distorting practices.

The full array of such destructive activities probably damages our economy to a significant degree. Foreign economic espionage by itself is a significant factor only in particular cases. Overall, it probably matters at the margin. Thus, economic counterintelligence is not likely to prove a panacea for US economic problems. Nevertheless, considering that economic success or failure is often determined at the margin, (b)(1) a vigorous economic CI program could yield valuable positive results.

Looking Ahead

In the future, monitoring and assessing the foreign intelligence threat to US economic interests are likely to assume greater importance for the US Intelligence Community. Fulfilling our responsibility in this area will be a challenge. Conceptualizing the issues will continue to be complex, as we try to define what activities constitute espionage, and seek policy guidance about what interests are "American"—considering the multinational ownership of many corporations, for example. We will need to surmount any conscious or subconscious tendency to apply a double standard, which could lead us to play down hostile activities if conducted by traditional allies. At the same time, we will need to avoid the pitfall of hyping the threat as a means of justifying bureaucratic budgets, satisfying a longing for new "enemies" to replace the old, or rationalizing our national economic problems.

Definitions and Counterintelligence Functions in the Economic Area

Economic counterintelligence is the monitoring, through human or technical means, of foreign targeting of classified information, or clandestine collection of proprietary information, that enhances a foreign country's economic competitiveness *vis-a-vis* the US. This term also encompasses attempts to counter such espionage activity. We have traditionally emphasized tracking the theft of classified material, but we also monitor acquisition of business information. In the past our CI monitoring has focused largely on activities conducted or coordinated by foreign intelligence organizations. But our coverage now includes collection involving other components of foreign governments, as well as operations conducted by foreign companies.

Economic espionage is government-sponsored intelligence collection conducted for the purpose of enhancing a country's economic competitiveness.

(b)(1)

Industrial or *commercial espionage* is the theft, either by a government or by a company, of business information that is proprietary in nature but not classified, for the purpose of giving particular firms an edge in international competition. We do not engage in commercial espionage ourselves.

(b)(1)
(b)(3)(n)

This article is classified ~~SECRET~~ (b)(3)(n)

(b)(3)(n)